REMARKS

This amendment is responsive to the Final Office Action dated July 22, 2005. Applicants have made no claim amendments. Claims 1, 2, 4-9 and 12-20 remain pending.

Claim Objections

In the Office Action, the Examiner objected to Applicants' amendment filed 04-04-2005. In particular, the Examiner stated that the limitation of "discarding at least a portion of the decrypted unauthenticated packet application data for the security record prior to receiving a final packet of the security record" is not taught by the specification.

In general, Applicants refer the Examiner to the "bufferless approach" described within pages 26 and 27 of the present application. In this embodiment, the intermediate acceleration device described by the Applicants uses "little or no buffer" when decrypting, forwarding and authenticating application data. For example, line 6 of page 26 first states that a "bufferless or small buffer approach" is used in one embodiment to handle a multisegment problem. Page 26, ll. 8-10 goes on to state:

> *In the bufferless approach, individual segments of multisegment SSL records are decrypted, but not authenticated prior to being sent to the server. Upon receipt of the last segment in the series (packet 3 in the above example), the data will be authenticated, however, individual segments are not.*

This portion make clear that, in this embodiment, the acceleration device decrypts individual SSL records and sends the decrypted data to the server prior to authentication. Moreover, this makes clear that authentication is not performed for individual segments, and does not occur until the last segment of the security record is received.

Further, page 26, ll. 12-14 states that the bufferless approach "reduces the hardware requirements of the device be requiring little or no buffer memory allocated to multi segment SSL packets." Thus, the present specification would be clear to one of ordinary skill that, in the bufferless and small buffer embodiments, the individual segments of an SSL record are not buffered, i.e., discarded, and that authentication does not occur until the last segment of that SSL record is subsequently received. Consequently, the limitation "discarding at least a portion of the decrypted unauthenticated packet application data for the security record prior to receiving a final

packet of the security record" accurately represents the buffered and small buffer embodiments described and taught by the specification.

Claim Rejection Under 35 U.S.C. § 103

In the Final Office Action, the Examiner rejected claims 1, 2 and 4 under 35 U.S.C. 103(a) as being unpatentable over Jardin (USPN 6,681,327) in view of Scholnick (USPN 5,978,918). The Examiner rejected claim 6 as inherent in any SSL communication. Finally, the Examiner rejected claims 5, 7-9 and 12-20 under 35 U.S.C. 103(a) as being unpatentable over Jardin in view of Scholnick in further view of Narad et al. (6,157,955).

Applicants respectfully traverse the rejection. The applied references fail to disclose or suggest the inventions defined by Applicants' claims, and provide no teaching that would have suggested the desirability of modification to arrive at the claimed invention.

Claims 1, 2 and 4-6

Applicants claim 1 requires discarding at least a portion of the decrypted, unauthenticated packet application data for the security record prior to receiving a final packet of the security record. In this manner, claim 1 is directed to the bufferless or small buffer embodiment described above. Neither Jardin nor Scholnick teach or suggest these or other elements of claim 1.

With respect to claim 1, the Examiner previously acknowledged that Jardin fails to teach or suggest authenticating decrypted packet application data of a security record on receipt of a final packet of the security record. In the current Action, the Examiner acknowledged that Jardin fails to teach or suggest discarding at least a portion of the decrypted, unauthenticated packet application data for the security record prior to receiving a final packet of the security record.

However, the Examiner asserts that Scholnick discloses "discard[ing] a portion of the packet data prior to receiving the final packet segment and authenticating the data." Even before looking to Scholnick, Applicants point out that the Examiner has misquoted Applicants' claim 1. Claim 1 requires discarding a portion of application data for a security record before receiving a final packet of that security record. Claim 1 then requires that that same security record be authenticated after the final packet is received, i.e., after a portion of that security record has been discarded. These elements are literally required by claim 1, and the Examiner's statement that

Scholnick discloses "discard[ing] a portion of the packet data prior to receiving the final packet segment and authenticating the data" is a gross mischaracterization of these elements of Applicants' claim 1.

Moreover, Scholnick fails to disclose or suggest even the features suggested by the Examiner. Scholnick describes a security process involving a consumer and a transaction processor. The consumer receives "private data" from a transaction processor, encrypts a verification and sends a verification to the TP over a public network or the nonpublic network. The TP receives the verification, discards the private data that was sent to the receiver, and passes the verification to the retailer over either the public network or the nonpublic network.[1]

Scholnick fails to teach or suggest the elements of Applicants' claim 1 for numerous reasons. Most fundamentally, the transaction processor and the consumer of Scholnick "discard" private data after a transmission of the private data has been verified, thus "authenticating" the sender. Schonlick clearly states the private data is discarded after authentication. Thus, Schonlick does not teach or suggest discarding at least a portion of the decrypted, unauthenticated packet application data for the security record prior to receiving a final packet of the security record, as required by claim 1. In Scholnick, the private data is discarded after a verification is received that authenticates the consumer, not prior to authentication, as required by claim 1. Thus, Jardin in view of Scholnick fails to teach or suggest these elements of claim 1.

With respect to claim 4, neither Jardin nor Scholnick teach or suggest buffering the remaining portion of the packet application data as a minimal length sufficient to complete a block cipher used to encrypt the data. In fact, neither Jardin nor Scholnick even suggest buffering just a remaining portion (i.e., a non-discarded portion) of application data. The Examiner admits that Jardin fails to teach discarding any portion of a security record at all. This is prima facie evidence that his assertion that Jardin teaches buffering a *remaining portion* is incorrect. As neither Jardin nor Scholnick teach or suggest discarding at least a portion of the decrypted application data for a security record prior to authentication of that security record, the references clearly fail to teach or suggest buffering only a *remaining portion of application for a security record* having a minimal length sufficient to complete a block cipher used to encrypt the data, as required by claim 4. Applicants refer the Examiner to the "small buffer" embodiment

[1] Scholnick at col. 5, ll. 13-40.

described above. None of the references teach or suggest only storing partial application data for a security record prior to authentication of that security record, as required by Applicants' claim 1.

The Examiner's rejection of claim 5 is very confusing. With respect to claim 5, the Examiner states that "The combination of Jardin and Scholnick does not explicitly explain a packet authentication." If this were true, how does the Examiner reject claim 1 based on Jardin and Scholnick, since claim 1 specifically requires authentication of application data of security record? Moroever, the Examiner appears to be confusing Applicants' claim 5 with verifying the contents of a packet, which is entirely incorrect. As pointed out by the Applicants in their previous response, the "cryptographic key" referenced by the Examiner is described by Narad in reference to cryptographic unit that generally supports encryption and decryption. The "checksum" described by Narad and relied upon by the Examiner is used to determine whether a packet contents is valid or corrupted in some form. Narad makes no mention of authenticating a security record or authenticating application data that spans multiple packets at all.

In any event, with respect to claim 5, Applicants point out that none of the references teach or suggest authenticating includes authenticating the decrypted data for the security record upon receiving a final TCP segment of a multi-segment encrypted data stream and after forwarding the decrypted, unauthenticated application data received prior to the final TCP segment. Claim 5 specifically requires that the decrypted data of a security record is authenticated **after** the TCP data received prior to the last TCP segment for that same record has **already been forwarded**. As explained above with respect to claim 1, none of the references, either singularly or in combination, teach or suggest an acceleration device that forwards application data of a security record to server prior to authenticating subsequent application data of that same security record. The cited portions of Narad are irrelevant.

With respect to claim 6, the Examiner argues that the elements of Applicants' claims are inherent in any SSL-based communication by an intermediary apparatus. However, the Examiner overlooks that claim 6 requires notifying the client apparatus if a failure in authenticating the security record occurs after forwarding the decrypted, unauthenticated application data to the server. There is nothing to suggest that conventional SSL-based intermediary acceleration devices issue an error notification after forwarding the decrypted,

unauthenticated application data. Applicants point out that, in the context of Applicants' bufferless or small buffer embodiment, the application data is forwarded prior to authentication, thereby possible reducing or minimizing hardware buffering requirements (see discussion of claim 1 above). Claim 6 is directed to the unique step that, in such an embodiment, an error notification is issued to the client after forwarding the data. Thus, even though the data has already been forwarded to the server, an error message is nevertheless issued to the client. Presumably, the "bad_record_mac" referred to by the Examiner occurs in conventional systems at the time of authentication which, as demonstrated by Jardin and the other references, is prior to forwarding any of the application data from an intermediate device to a server.

Claims 7-9, 12-15

With respect to claim 7, it appears the Examiner failed to even address the required elements of buffering a portion of the decrypted application data and discarding a remaining portion. In fact, the Examiner failed to even comment on these elements that were added by Applicants' previously filed amendment.

Moreover, as explained above with respect to claim 1, none of the references teach or suggest buffering only a portion of decrypted application data and discarding a remaining portion prior to authenticating the application data when the information for authenticating the application data is received in the last of the multiple packets.

Further, the Examiner appears to recognize that Jardin does not teach or suggest authentication of application data when the information for authenticating the application data is received in the last of the multiple packets. Again the Examiner appears to confuse authentication of application data (i.e., authentication of the sender) with verification of the packets contents. In an attempt to overcome the deficiencies of Jardin, the Examiner refers to the "checksum" described by Narad and states that one would be motivated to identify and discard packets that have been altered or modified.

The Examiner fails to consider that claim 7 specifically requires forwarding the decrypted data and then discarding a portion of it. In other words, a portion of the "good" data that is forwarded by the intermediary device is nevertheless discarded prior to authentication to reduce buffering requirements. The fact that Narad teaches a checksum to discard altered or modified

packets is irrelevant as those packets would not constitute application data forwarded by the intermediate device and subsequently discarded, as required by claim 7.

Consequently, neither Jardin nor Narad, either separately or in combination, teach or suggest forwarding decrypted application data, buffering a portion of the decrypted application data and discarding a remaining portion of that same decrypted application data prior to authenticating the application data, and authenticating the remaining application data when the information for authenticating the application data is received in the last of the multiple packets, as required by Applicants' amended claim 7.

With respect to claim 12, neither Jardin nor Narad teach or suggest buffering the remaining portion of the packet application data as a minimal length sufficient to complete a block cipher used to encrypt the data. As discussed above with respect to claim 4, neither Jardin nor Narad even suggest buffering just a remaining portion (i.e., a non-discarded portion) of application data that has already been forwarded to a server by an intermediary device. As none of the references teach or suggest discarding at least a portion of the decrypted application data for a security record prior to authentication of that security record, the references clearly fail to teach or suggest buffering only a *remaining portion of application data already forwarded to a server, wherein the remaining portion has* a minimal length sufficient to complete a block cipher used to encrypt the data, as required by claim 12. Applicants refer the Examiner to the "small buffer" embodiment described in the present application. None of the references teach or suggest only storing partial application data of a minimal length after forwarding the decrypted application data and prior to authentication of that application data, as required by Applicants' claim 12.

With respect to claim 15, the Examiner again argues that the elements of Applicants' claim 15 are inherent in any SSL-based communication by an intermediary apparatus. However, the Examiner again overlooks that claim 15, when viewed properly with respect to independent claim 7, requires generating a reset to the first system if authentication fails after forwarding the decrypted, unauthenticated application data to the second system. There is nothing to suggest that conventional SSL-based intermediary acceleration devices issue a reset after forwarding the decrypted, unauthenticated application data. Applicants point out that, in the context of Applicants' bufferless or small buffer embodiment, the application data is forwarded prior to

authentication, thereby possible reducing or minimizing hardware buffering requirements. Claim 15 is directed to the unique step that, in such an embodiment, a reset is issued to a first system after forwarding the data to a second system. Thus, even though the data has already been forwarded from an intermediate device to a second device, a reset is nevertheless issued to the first device. Presumably, the "bad_record_mac" referred to by the Examiner occurs in conventional systems at the time of authentication which, as demonstrated by Jardin and the other references, is prior to forwarding any of the application data from an intermediate device.

Claims 16-20

With respect to claim 16, Jardin fails to teach or suggest buffering encrypted data in a memory buffer in a device, the buffer having a length equivalent to a block cipher size necessary to perform the cipher. In rejecting claim 16, the Examiner again cited Jardin at col. 6, ll. 9-14. However, this passage of Jardin clearly states that the broker of the Jardin system buffers incoming application data "until a handshake can be used to establish a data transport connection between the broker 120 and the server 130a."

The Examiner has failed to identify any portion of Jardin that discusses an actual buffer size, let alone any correlation between the buffer size and the block cipher size. Moreover, given that the buffer Jardin is to store incoming application data until a data transport connection can be established, Jardin clearly suggests that the buffer is extremely large, unrelated to the block cipher size and, therefore, not "equivalent to the block cipher size necessary to perform the cipher," as required by Applicants' claim 16. Thus, in contrast to the Examiner's assertion, Jardin fails to teach or suggest a method for providing secure communications using limited buffer memory that includes a buffer having a length equivalent to a block cipher size necessary to perform the cipher, as required by Applicants' claim 16.

Claim 19 requires authenticating the data on receipt of a final segment of the encrypted data after forwarding the unauthenticated application data that is received prior to the final segment. Thus, claim 19 specifically requires the step of authenticating the data only: (1) on receipt of the final segment of the encrypted data, and (2) after forwarding any of that same data that is received prior to the last segment.

With respect to claim 19, the Examiner again argues that Narad teaches using a checksum to discard altered packets. However, this argument fails to recognize that Applicants' claim

requires discarding all of the application data that has already been forwarded by the intermediate device and received prior to the last segment, i.e., even any non-altered or unmodified (i.e., "good") application data that was received prior to the last segment. Thus, use of Narad's checksum to discard bad packets does not anticipate these elements.

For at least these reasons, the Examiner has failed to establish a prima facie case for non-patentability of Applicants' claims 1, 2, 4-9 and 12-20 under 35 U.S.C. 103(a). Withdrawal of this rejection is requested.

CONCLUSION

All claims in this application are in condition for allowance. Applicants respectfully request reconsideration and prompt allowance of all pending claims. Please charge any additional fees or credit any overpayment to deposit account number 50-1778. The Examiner is invited to telephone the below-signed attorney to discuss this application.

Date: October 17, 2005

By: Kent J. Sieffert

SHUMAKER & SIEFFERT, P.A.
8425 Seasons Parkway, Suite 105
St. Paul, Minnesota 55125
Telephone: 651.735.1100
Facsimile: 651.735.1102

Name: Kent J. Sieffert
Reg. No.: 41,312